REMARKS/ARGUMENTS

In the Office Action, the Examiner noted that claims 1-27, 56-64, and 66-83 are pending in the application. The Examiner additionally stated that claims 1-27, 56-64, and 66-83 are rejected. By this communication, claims 23, 26, and 77-78 are cancelled and claims 1, 13, 24-25, 27, 56, 79, and 81-82 are amended. Hence, claims 1-22, 23-25, 27, 56-64, 66-76, and 79-83 are pending in the application.

Applicant hereby requests further examination and reconsideration of the application, in view of the foregoing amendments.

Response to Allegation that Applicant Did Not Adequately Traverse Declaration of Official Notice in Previous Office Action

The Examiner noted that because Applicant did not adequately traverse the declaration of Official Notice from the previous Office Action (see page 9, at #13), these declarations are now taken as admissions of prior art, as per MPEP 2144.03(c).

Applicant responds by asserting that the Examiner's rejection in the previous Office Action of claims 12 and 66 was indeed traversed, in whole, by Applicant in the Reply of 08/04/2007. Applicant's traversal contemplated all stated reasons for rejection, including the Examiner's Official Notice. For ease of reference, Applicant provides below the noted traversal from the Reply of 08/04/2007, at page 21, first paragraph:

> *The Examiner also rejected claims 12 and 66 under 35 U.S.C. 103(a) as being unpatentable over Kessler.* ***Applicant traverses*** *and notes that claims 12 and 66 depend from claims 1 and 56, respectively, and add further limitations over that subject matter* ***which is argued above*** *as being allowable over the prior art of record. Accordingly, Applicant respectfully requests that the Examiner withdraw the rejections of claims 12 and 66.*

In footnote 1 of the instant Office Action, the Examiner opined that Applicant's traversal of the rejections of claims 12 and 66 is inadequate insofar as the traversal was limited to

asserting that the claims should be allowable by merit of Applicant's belief that the parent claims should also be allowable.

In reply, Applicant respectfully submits that arguments provided in traversal of the rejections of claims 1 and 56 support the traversal of the Official Notice in that Applicant argued in the reply of 08/04/2007 that a co-processor cannot be considered equivalent to a general purpose microprocessor.

More specifically, Applicant argued that the invention of claims 1 and 56 is directed towards performing cryptographic operations within a *microprocessor*, analogous to Kessler's host processor 202, where those operations are prescribed by a macro instruction that is programmed within an instruction flow that is fetched from memory by fetch logic in the *microprocessor*, and that Kessler does not teach fetch logic, configured to fetch an instruction flow from memory for execution by a *microprocessor*. Furthermore, Applicant argued that Kessler does not teach that the instruction flow includes a cryptographic instruction that prescribes a cryptographic operation, and that Kessler does not teach or suggest that such an instruction be provided to allow his host processor to perform the noted security functions. This is because Kessler teaches that it is desirable to provide a *co-processor* to perform such functions.

Consequently, it is respectfully submitted that Applicant's arguments in the reply of 08/04/2007 are sufficient to distinguish a microprocessor from a co-processor, and thus the Examiner's Official Notice that the cryptographic apparatus of Miller (US 5134713) would be prescribed according to the x86 instruction format to facilitate its use with a common x86 host processor was adequately overcome by Applicant's traversal noting that claims 12 and 66 add further limitations over that subject matter *which was argued* therein as being allowable over the prior art of record.

Applicant wishes to respectfully add that Miller (US5134713) does not teach, suggest, allude to, or even hint at cryptographic apparatus. Miller teaches an 80387 floating point co-processor.

In view of the above points, Applicant respectfully submits that the declarations made by the Examiner in the noted Official Notice have been adequately traversed and are thus not to be considered as prior art.

Information Disclosure Statements

The Examiner suggested that in the future, Applicant may wish to expedite the examination process by refraining from submitting redundant IDS forms all listing the same reference (the Examiner cited the five IDS submissions of 5/23 and 5/24) as well as consolidating multiple references to be considered onto one IDS form (see the multiple IDS forms, all filed 5/31/07, each listing different references).

Applicant apologizes for the five submissions of 5/23 and 5/24 listing the same reference. Upon investigation, it was found that an error within facsimile reception services at the time precluded the undersigned from receiving the auto-reply page from USPTO central fax services and in an effort to ensure that the Examiner was provided with material references for examination of the instant application under the undersigned's duty of candor and good faith, the same IDS was faxed to the PTO until it was determined with certainty that it had been received.

In reply to the Examiner's suggestion for consolidation of multiple IDS forms filed on the same day, Applicant responds that it is the practice of the undersigned to provide references that have been cited in related and foreign cases for examination of the instant application in as timely a manner as practicable. Applicant will, however, make every effort within reason to refrain from submitting more than one IDS in a single day.

In the Specification

Applicant has amended the specification to secure a substantial correspondence between the claims amended herein and the remainder of the specification. No new matter is presented.

In the Claims

Rejections Under 35 U.S.C. §102(e)

The Examiner rejected claims 1-6, 11, 23-27, 56-60, and 77-83 under 35 U.S.C. 102(e) as being anticipated by Kessler et al., U.S. Patent 6,789,147 (hereinafter, Kessler). Applicant respectfully traverses the Examiner's rejections.

Regarding claims 1 and 56, the Examiner noted that Kessler discloses a (microprocessor) apparatus for performing cryptographic operations comprising: fetch logic, configured to fetch an instruction flow from memory for execution by a microprocessor (col. 4, line 59-col. 5, line 36), said instruction flow comprising an instruction, configured to direct said microprocessor to perform the cryptographic operation (col. 4, lines 10-16; col. 5, lines 29-36; Figure 7), wherein said cryptographic instruction prescribes one of the cryptographic operations (Figure 3); said cryptographic operation comprising: an opcode field, configured to prescribe that the circuit accomplish the cryptographic operation as further specified within a control word stored in a memory (element 302 of Fig. 3; col. 5, lines 37-50); and a repeat prefix field, coupled to said opcode field, configured to indicate that the cryptographic operation prescribed by the cryptographic instruction is to be accomplished on a plurality of blocks of input data (element 310 of Fig.3; col. 5, line 50 - col. 6, line 10).

In reply to arguments submitted by Applicant in the reply of 08/04/2007, the Examiner stated that Applicant's arguments filed 8/4/07 have been fully considered but they are not persuasive. The Examiner referred to page 19 of the amendment of 8/4/07, noting that Applicant primarily argues that the instant invention differs from the prior art in that the prior art discloses the use of a cryptographic co-processor, rather than a microprocessor, to execute the recited instruction. The Examiner then opined that this is an artificial distinction as the co-processor is itself a microprocessor and referred Applicant to a "definition" of the word coprocessor from one of three results obtained by searching dictionary.com via the internet. The particular result the Examiner relied upon is taken from American Heritage Dictionary.

The "definition" result relied upon by the Examiner reads as follows:

> *co·proc·es·sor (kō'prŏs'ĕs-ər) Pronunciation Key*
>
> *n. A microprocessor that performs specialized functions that the central processing unit cannot perform or cannot perform as well and as quickly.*

From this result the Examiner inferred equivalence between a microprocessor and a co-processor. The Examiner further opined that the is nothing in the claims that would preclude the claimed microprocessor from being utilized as a co-processor in a more complex computer system and noted with respect to the new limitations of claims 1 and 56 that the ability of a microprocessor to fetch an instruction flow (i.e. a computer program) from memory has been inherent to microprocessors in general since well nigh time immemorial (see the Von Neumann Architecture reference), but that Kessler nevertheless explicitly discloses wherein the coprocessor is capable of retrieving an instruction flow (i.e., a macro security operation comprising a plurality of primitive security operations: col. 4, lines 10-16 & Figure 7) from a memory queue (further imparting the proper order, or flow, of execution of said instructions, col. 5, lines 8-17), and wherein each of the primitive instructions being executed has the opcode and prefix field as identified from the previous Office Action.

Applicant respectfully disagrees with the Examiner's characterization of claims 1 and 56 and of the teachings of Kessler for the following reasons.

First, Applicant agrees with the Examiner that one of the fundamental issues that distinguishes the present invention from the prior art is that the prior art discloses the use of a cryptographic co-processor (as is taught by Kessler), but the present invention contemplates performance of cryptographic operations in a microprocessor. However, Applicant adamantly submits that a co-processor cannot by any sense of the word be held analogous to a microprocessor as is taught within the instant disclosure. One skilled in the art will profess without wavering that any reasonable definition of a co-processor would comprehend a separate device for which special purpose operations are off-loaded from the main microprocessor. Applicant also respectfully submits that such a distinction if far from "artificial" as is put forth by the Examiner and to provide support for this

assertion, Applicant herewith provides another of the three results obtained from searching dictionary.com for "co-processor." The following result is taken from the Free On-line Dictionary of Computing:

> *Coprocessor*
>
> *Any computer processor which assists the main processor (the "CPU") by performing certain special functions, usually much faster than the main processor could perform them in software. The coprocessor often decodes instructions in parallel with the main processor and executes only those instructions intended for it. The most common example is a floating point coprocessor (or "FPU"), others are graphics and networking.*

Applicant also provides a definition of "coprocessor" taken from Wikipedia along with a distinguishing definition of "microprocessor" as follow:

> *A **coprocessor** is a computer processor used to supplement the functions of the primary processor (the CPU). Operations performed by the coprocessor may be floating point arithmetic, graphics, signal processing, string processing, or encryption. By offloading processor-intensive tasks from the main processor, coprocessors can accelerate system performance. Coprocessors allow a line of computers to be customized, so that customers who do not need the extra performance need not pay for it.*
>
> *A **microprocessor** incorporates most or all of the functions of a central processing unit (CPU) on a single integrated circuit (IC).*

Accordingly, Applicant submits that it is not an artificial distinction to incorporate the capability to perform cryptographic operations into a microprocessor that performs most of all of the functions of a central processing unit on a single integrated circuit, for the instant disclosure clearly teaches that the microprocessor according to the present invention provides those functions. In many places the instant disclosure refers to the apparatus within the microprocessor provided to fetch instructions in a application program from memory, to access registers, to perform address translation, to load variables, to store results, and to perform, in some embodiments, integer operations

prescribed by integer instructions in the application program, to perform floating point operations (i.e., floating point arithmetic) prescribed by floating point instructions in the application program, and *to perform cryptographic operations prescribed by a cryptographic instruction in the application program.*

Thus, Applicant respectfully submits that the instant disclosure stands alone to support the distinction between a co-processor and a microprocessor and that such a distinction is significantly and is patentably distinct. In fact, paragraph [0017] of the instant disclosure notes limitations associated with the "co-processor" approach taught by Kessler by stating, "cryptographic co-processor implementations are additionally vulnerable to snooping because the data channel is not on the same die as the host microprocessor." Thus in paragraph [0018] Applicant proposes that there is "a need for dedicated cryptographic hardware within a present day microprocessor such that an application program that requires a cryptographic operation can direct the microprocessor to perform the cryptographic operation via a single, atomic, cryptographic instruction." The remainder of the specification and claims provide such a technique for addressing this long-felt need.

Having stated the above, Applicant notes that Kessler clearly teaches a co-processor 212 (i.e., a computer processor which assists the main processor by performing certain special functions) that is configured to receive requests to perform security operations (i.e., the special functions) over a system bus 210, where the request are provided by a host processor 202. (See Abstract, Fig. 2, and col. 4, line 41 through col. 5, line 36) Kessler's invention is provided to offload a portion of the processing that the host processor must perform in order to perform the noted security operations. Kessler's co-processor clearly performs only those special security operations and is not capable of performing those operations normally attributed to a microprocessor. To support this clear distinction, Applicant provides an excerpt from Kessler that certainly teaches away from the technique taught by Applicant as is recited in claims 1 and 56:

Performing the tasks to establish a secure session is *processor intensive* (that is, intensive for a host processor). If *a general purpose processor*, acting as the host processor for a

network element, performs these tasks, then the network element's system performance will suffer because resources will be consumed for the tasks. . . . Coprocessors have been developed to offload some of the tasks from the host processor. . . One aspect of the invention is the communication of tasks and results between *a host processor and a security coprocessor*, where the coprocessor has multiple execution units. Another aspect of the invention is the type of tasks, specifically macro security operations, that can be transferred by a host processor to a security coprocessor, where the coprocessor has multiple execution units. (col. 1, line 56 – col. 2, line 10; col. 4, lines 19-23) In addition, Kessler teaches a host processor 202, host memory 204, a coprocessor 212 that are coupled via a system bus 210. (col. 4, lines 44-47)

In contrast, Applicant's invention, as recited in amended claims 1 and 56, is directed towards performing cryptographic operations within a microprocessor, analogous to Kessler's host processor 202, where those operations are prescribed by a macro instruction that is programmed within an instruction flow (i.e., an application program) that is fetched from memory by fetch logic in the microprocessor. Applicant agrees with the Examiner's remark that a co-processor can fetch instructions from memory, but notes that such a limitation was provided to support the distinction that the microprocessor according to the present invention is a general purpose CPU that additionally incorporates the capability to perform cryptographic operations responsive to a cryptographic instruction embedded in an application program. To further clarify this point, Applicant has amended claim 1 to more clearly point out the aforementioned elements in contrast to the that which is taught by Kessler, that is, a co-processor. Clearly, Kessler does not teach a cryptography unit in parallel with an integer unit disposed within execution logic in a microprocessor, that operate in parallel to perform both cryptographic rounds and integer operations, both required to perform the cryptographic operation *within the microprocessor*. Applicant also asserts that the cryptographic operation is performed *atomically* responsive to *a cryptographic instruction*, as opposed to a plurality of primitives, which is taught by Kessler.

Regarding claim 56, Applicant provides amendments to recite translation logic and a cryptography unit, both within the microprocessor, and notes again that Kessler's

apparatus for performing the security operations is on a separate security co-processer that communicates with a host processor over a system bus.

In view of the above points, Applicant respectfully requests that the rejections of claims 1 and 56 be withdrawn.

By this communication, claims 23, 26, and 77-78 are cancelled, thereby rendering the rejections moot.

With respect to claims 2-6, 11, 24-25, 27, 57-60, and 79-83, these claims depend from claims 1 and 56 as appropriate, and add further limitations that are neither anticipated nor made obvious by Kessler. Accordingly, Applicant respectfully requests that the Examiner withdraw the rejections of claims 2-6, 11, 24-25, 27, 57-60, and 79-83.

Rejections Under 35 U.S.C. §103(a)

The Examiner rejected claims 7-10 and 61-64 under 35 U.S.C. 103(a) as being unpatentable over Kessler, as noted above, and further in view of "Applied Cryptography, 2nd Edition."

Applicant respectfully traverses the Examiner's rejections and notes that claims 7-10 and 61-64, depend from claims 1 and 56, respectively, and add further limitations over that subject matter which is argued above as being allowable over the prior art of record. Accordingly, Applicant respectfully requests that the Examiner withdraw the rejections of claims 7-10 and 61-64.

The Examiner also rejected claims 12 and 66 under 35 U.S.C. 103(a) as being unpatentable over Kessler. Applicant traverses and notes that claims 12 and 66 depend from claims 1 and 56, respectively, and add further limitations over that subject matter which is argued above as being allowable over the prior art of record. Accordingly, Applicant respectfully requests that the Examiner withdraw the rejections of claims 12 and 66.

The Examiner additionally rejected claims 13-22 and 67-76 under 35 U.S.C. 103(a) as being unpatentable over Kessler and further in view of Johns-Vano et al. (U.S. Patent 6,026,490). Applicant respectfully traverses and notes that claims 13-22 and 67-76

depend from claims 1 and 56, respectively, and add further limitations over that subject matter which is argued above as being allowable over the prior art of record. Accordingly, Applicant respectfully requests that the Examiner withdraw the rejections of claims 13-22 and 67-76.

CONCLUSIONS

Applicant believes this to be a complete response to all of the issues raised in the instant office action and further submits, in view of the amendments and arguments advanced above, that claims 1-22, 23-25, 27, 56-64, 66-76, and 79-83 are in condition for allowance. Reconsideration of the rejections is requested, and allowance of the claims is solicited.

Applicant also notes that any amendments made by way of this response, and the observations contained herein, are made solely for the purpose of expediting the patent application process in a manner consistent with the PTO's Patent business Goals (PBG), 65 Fed. Reg. 54603 (September 8, 2000), and are furthermore made without prejudice to Applicant under this or any other jurisdictions. It is moreover asserted that insofar as any subject matter might otherwise be regarded as having been abandoned or effectively disclaimed by virtue of amendments made herein and/or incorporated in attachments submitted with this response, Applicants wishes to reserve the right and hereby provides notice of intent to restore such subject matter and/or file a continuation application in respect thereof.

Applicant earnestly requests that the Examiner contact the undersigned practitioner by telephone if the Examiner has any questions or suggestions concerning this amendment, the application, or allowance of any claims thereof.

I hereby certify under 37 CFR 1.8 that this correspondence is being facsimile transmitted to the United States Patent and Trademark Office on the date of signature shown below.

Respectfully submitted,
HUFFMAN PATENT GROUP, LLC

/Richard K. Huffman/

By: _____

RICHARD K. HUFFMAN, P.E.
Registration No. 41,082
Tel: (719) 575-9998

03/09/2008

Date: _____